Information Technology (IT) Resources Acceptable Use Standard

Issue Date: June 1, 2004
Effective Date: June 1, 2004

Number: HHSS-2004-003-A

1.0 Purpose

Define acceptable use of IT resources, which include but are not limited to computer assets, electronic communication, HHSS Data Communication Network, data applications, and any proprietary hardware used to process data on the network.

2.0 Scope

This standard applies to employees, contractors, consultants, temporaries, and other workers employed by HHSS including all personnel affiliated with third parties. It is the responsibility of every Information Technology resource user to know these guidelines and act accordingly.

3.0 Standard

This standard provides guidelines for compliance to the IT Resources Acceptable Use Policy No. HHS 2004-003.

3.1 Computer Assets

Computer assets are defined as desktop computers, servers, laptop computers, PDA (personal digital devices), mainframe computers, printers, routers, switches, hubs, portable storage devices, digital cameras, and any other electronic device that creates, stores, processes, and exchanges HHSS information created, stored, contracted or managed by HHSS.

3.1.1 HHSS employees and contracted agents are responsible for the reasonable care and protection of the computer assets assigned to them and for meeting all policies and standards governing their use.

3.1.2 Acceptable use of computer assets provided by HHSS is limited to actions and transactions necessary for the performance of State business.

3.1.3 Computer assets used by HHSS employees and contracted representatives to perform HHSS business activities must be owned, leased, or managed by HHSS and meet specifications and requirements published by the Information Systems and Technology division (IS&T) of Finance and Support, and approved by IS&T for agency use.

3.2 HHSS Data Communication Network (LAN, WAN, Internet/Intranet/Extranet)

HHSS Data Communication Network (HDCN) is defined as the Local Area Network (LAN) and Wide Area Network (WAN), owned, contracted, or managed by HHSS, and Internet/Intranet/Extranet access owned, supported, contracted, or managed by HHSS.

3.2.1 Acceptable use of the HDCN must be limited to actions and transactions necessary for the performance of State business.

3.2.2 HDCN access may not be used to perform any illegal activity such as trying to gain unauthorized access to restricted sites (hacking), harassment of any kind, creation of unauthorized Intranet sites or pages, sharing of copyrighted material, or the production of any material that may be deemed offensive.

3.2.3 Use of the HDCN to deliberately spread software viruses of any kind is strictly forbidden and may result in disciplinary action up to and including termination of employment.

3.2.4 HHSS employees and contracted agents are responsible for the reasonable protection and use of the HDCN access granted to them and must follow all security rules and standards defined and published by the IS&T Administrator or their agent.

3.2.5 HHSS IT resources may not be used for any unauthorized file sharing. Downloading any music, video, or software files in violation of copyright laws is prohibited and the employee will be held personally liable for any fines or judgments that may result from their actions.

3.2.6 No software, digital images, music, streaming video, radio transmissions, telephone transmission, or data files may be downloaded from the Internet without the approval of the IS&T Administrator or their agent.

3.3 Electronic Communication (E-mail, Instant Messaging, data exchange)

Electronic communication include e-mail, instant messages, electronic data exchange, and any other electronic method of exchanging information created, stored, contracted, or managed by HHSS.

3.3.1 All electronic communication is the property of HHSS and not the personal property of any individual. HHSS rules and regulations govern privacy and confidentiality of information contained in electronic communication.

3.3.2 Acceptable use of the electronic communication access provided by HHSS must be limited to actions and transactions necessary for the performance of State business. HHSS supports and enforces the State of Nebraska Data Communications Network Acceptable Use Policy standards and guidelines as stated in section 3.9 below. All other use is prohibited.

3.3.3 Deliberate spreading of software viruses of any kind is prohibited and may result in disciplinary action up to and including termination of employment.

3.3.4 Deliberate spreading of unsolicited E-mail or electronic messages (i.e., SPAM) is strictly prohibited and may result in disciplinary action up to and including termination of employment.

3.3.5 HHSS employees and contracted agents are responsible for the reasonable protection and use of the Electronic Communication access granted to them and must follow all security rules and standards published by the IS&T Administrator or their agent.

3.3.6 No Electronic Communication technology may be used by HHSS employees and contracted agents that is not provided by or approved by the IS&T Administrator or their agent.

3.4 Data Applications

Data Applications are defined as software applications created, owned, licensed, or managed by HHSS and used to create, store, retrieve, process, and maintain information owned, supported, contracted, or managed by HHSS.

3.4.1 Use of a software applications is restricted to state business only and is subject to all policies, procedures, privacy rules and regulations, and acceptable use guidelines implemented by the HHSS Agency, Division, or program area that owns or holds the license of the software application.

3.4.2 Use of a software application must meet all guidelines defined in the Software Acceptable Policy and Software Acceptable General Use and Home Use Standards (HHSS-2004-004, HHSS-2004-004-A, and HHSS-2004-004-B).

3.5 HHSS Electronic Information

Electronic Information is defined as any digital information or graphics owned, contracted, stored, retrieved, processed, or maintained and managed by HHSS.

3.5.1 Electronic information used by HHSS staff and agents in the course of doing business is the property of HHSS and is subject to all policies, procedures, privacy rules and regulations, and acceptable use guidelines that may be implemented by HHSS. It is the responsibility of the user to know and abide by rules governing access and use of this information.

3.5.2 Use of electronic information is restricted to State business only and is subject to all policies, procedures, privacy rules and regulations, and acceptable use guidelines implemented by the HHSS Agency, Division, or program area that owns or holds the license of the electronic information.

3.5.3 No electronic information may be copied, processed, or stored on personal computer assets (see section 3.0 above for definition of computer assets) without prior written authorization from the HHSS owner of the electronic information.

3.5.4 No electronic information may be copied or distributed in violation of any policies, procedures, privacy rules and regulations, and acceptable use guidelines implemented by the HHSS Agency, Division, or program area that owns or holds the license of the electronic information.

3.5.5 Accessing or attempting unauthorized access to EPHI (electronic protected health information), IRS FTI (Internal Revenue Service Federal Tax Information) or other HHSS protected private and confidential information for other than a required business "need to know" is prohibited.

3.6 Wireless Access and Wireless Devices

3.6.1 No HHSS employee or contracted partner may implement wireless technology to process any HHSS transactions without the review and approval of the IS&T Administrator or their agent.

3.6.2 Wireless access devices used by HHSS employees and contracted representatives for business activities must be owned or leased by HHSS and meet specifications and requirements published by the IS&T Administrator or their agent and must be approved for use by the IS&T Administrator or their agent.

3.6.3 Only IS&T authorized staff may install a wireless access device to the HHSS data network connection jack, port, PC, or other devices connected to the data network.

3.7 Security Safeguards

3.7.1 Access to the HHSS network and LAN is restricted to HHSS staff and contracted representatives who meet the requirements as defined in the IT Access Control Standards (HHSS 2004-002-C).

3.7.2 HHSS employees and contracted agents are responsible for the reasonable protection of the network access granted to the individual. No system access codes, logon ID's, or passwords may be loaned, shared, or otherwise released to any other internal or external individual except when authorized by the IS&T Administrator or their agent.

3.7.3 Compiling logs of user names, system access codes, logon ID's and password by any individual, group, or organization not authorized by the IS&T Administrator or their agent is strictly prohibited.

3.7.4 The use of generic logon usernames, system access codes, or logon ID's to access the HHSS network, LAN, e-mail system, or any business software application by HHSS employees or contracted representatives is prohibited.

3.7.5 Password assignment and usage must meet specifications defined in the IT Access Control Standard (HHSS 2004-002-C).

3.8 Remote Access

3.8.1 No remote access to the HHSS network, LAN, WAN, or any software application is permitted without the review and approval of the IS&T Administrator or their agent.

3.9 State Data Communications Network.

HHSS supports and enforces the State Of Nebraska Acceptable Use Standards and Guidelines for use of the State of Nebraska Data Communications Network (SDCN) as published by the Department of Administrative Services, Division of Communications. Acceptable uses include:

3.9.1 To communicate and exchange professional development information, including online discussion or debate of issues in a field of knowledge.

3.9.2 To provide and simplify communications with other state agencies, units of government, and citizens.

3.9.3 To exchange communications in conjunction with professional associations, advisory committees, standards activities, or other purposes related to the user's professional capacity.

3.9.4 To apply for or administer grants or contracts for work-related applications.

3.9.5 To carry out regular administrative communications in direct support of work related functions.

3.9.6 To announce new products or services within the scope of work-related applications.

3.9.7 To access databases or files for purposes of work-related reference or research material.

3.9.8 To post work-related questions or to share work-related information.

3.9.9 To communicate to children at home, teachers, doctors, day care centers, and baby sitters, to family members to inform them of unexpected schedule changes, and for other essential personal business. The use of the State's telecommunications systems for essential personal business shall be kept to a minimum and shall not interfere with the conduct of state business.

4.0 Enforcement

Should a violation of this IT Resource Acceptable Use Standard occur, the individual(s) who committed the violation will be personally liable for their actions or the actions taken by others due to their violation of this standard. Lack of knowledge of or familiarity with this policy shall not release an individual from such liability. Any employee found to have violated this policy may be subject to disciplinary action, as defined in the governing policy HHS 2004 -003

5.0 Revision History

HR Legal 3/12/2004

CCT Approval – 05/27/2004